



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/511,751	02/24/2000	Boby Joseph	99,815	5539

20306 7590 02/02/2004

MCDONNELL BOEHNEN HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
SUITE 3200
CHICAGO, IL 60606

EXAMINER

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

5

DATE MAILED: 02/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/511,751

Applicant(s)

JOSEPH ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 13-22, 25-28, 30-34, 36 is/are rejected.
- 7) ☒ Claim(s) 11, 12, 23, 24, 29 and 35 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, 36 are rejected under 35 U.S.C. 102(e) as being anticipated by Heer, U.S. Patent No. 5,999,629. Referring to claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, 36, Heer discloses a data encryption security module that comprises an information processing system (first network device, Fig. 1, 20), an access control system (second network device, Fig. 1, 40), and a subscriber terminal (third network device, Fig. 1, 200). The security modules of the information processing system (first network device) and the access control system generate a symmetrical key (first set of key material) that is used for encrypted communication between the two modules, which meets the limitation of the second network device being capable of communicating with the first network device using

Art Unit: 2132

security determined by the first set of key material. The symmetrical key is generated by the public encryption key and the private key (key extension) of the information processing system (Col. 4, lines 31-51). Further the security module of the access control system (second network device) and the subscriber security module (third network device) may share a respective symmetrical key (second key material) that will be unique to the pair as a result of the public key associated with the security module of the subscriber module (third network device) and a per-use randomly generated key (key extension) emanating from the access control system security module (second network device) (Col. 4, line 61- Col. 5, line 3).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer, U.S. Patent No. 5,999,629, in view of Mniszewski, U.S. Patent No. 4,731,840. Referring to claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, 34, Heer discloses a data encryption security module that comprises an information processing system (first network device, Fig. 1, 20), an access control system (second network device, Fig. 1, 40), and a subscriber terminal (third network device, Fig. 1, 200). The security modules of the information processing system (first network device) and the access control system generate a symmetrical key (first set of key material) that is used for encrypted communication between the two modules, which meets the limitation of the second network device being capable of

Art Unit: 2132

communicating with the first network device using security determined by the first set of key material. The symmetrical key is generated by the public encryption key and the private key (key extension) of the information processing system (Col. 4, lines 31-51). Further the security module of the access control system (second network device) and the subscriber security module (third network device) may share a respective symmetrical key (second key material) that will be unique to the pair as a result of the public key associated with the security module of the subscriber module (third network device) and a per-use randomly generated key (key extension) emanating from the access control system security module (second network device) (Col. 4, line 61- Col. 5, line 3). Heer does not disclose an encryption key threshold length. Mniszewski discloses a method for encryption and transmission of digital data wherein the DES encryption is used that has 64 bit encryption keys (Col. 1, lines 44-45), which meets the 64 bit threshold limitation. It would have been obvious to one of ordinary skill in art at the time the invention was made to use DES encryption in the data encryption security module of Heer because DES encryption is the US standard cryptosystem as taught in Mniszewski (Col. 1, lines 31-35).

5. Claims 10, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer, U.S. Patent No. 5,999,629, in view of Tatebayashi, U.S. Patent No. 5,124,117. Referring to claims 10, 22, Heer discloses a data encryption security module that comprises an information processing system (first network device, Fig. 1, 20), an access control system (second network device, Fig. 1, 40), and a subscriber terminal (third network device, Fig. 1, 200). The security modules of the information processing system (first network device) and the access control system generate a symmetrical key (first set of key material) that is used for encrypted communication between the two modules, which meets the limitation of the second network device being capable of

Art Unit: 2132

communicating with the first network device using security determined by the first set of key material. The symmetrical key is generated by the public encryption key and the private key (key extension) of the information processing system (Col. 4, lines 31-51). Further the security module of the access control system (second network device) and the subscriber security module (third network device) may share a respective symmetrical key (second key material) that will be unique to the pair as a result of the public key associated with the security module of the subscriber module (third network device) and a per-use randomly generated key (key extension) emanating from the access control system security module (second network device) (Col. 4, line 61- Col. 5, line 3). Heer does not disclose that the computed keys could be a Diffie-Hellman key. Tatebayashi discloses a cryptographic key distribution system that uses DES encryption standards and Diffie-Hellman keys (Col. 2, lines 21-68). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use Diffie-Hellman keys in the data encryption module of Heer in order to provide secure communications as taught in Tatebayashi (Col. 1, lines 26-38).

Allowable Subject Matter

6. Claims 11, 12, 23, 24, 29, 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: The prior art does not disclose using the hash of an internal key and network device identifier, specifically a software serial number, as a key extension.

Conclusion

Art Unit: 2132

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684.


The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.



Benjamin E. Lanier



GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100